PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G11B 20/00, G06F 1/00

A1

(11) Numéro de publication internationale: WO 00/17871

(43) Date de publication internationale: 30 mars 2000 (30.03.00)

(21) Numéro de la demande internationale: PCT/FR99/02267

(22) Date de dépôt international: 23 septembre 1999 (23.09.99)

(30) Données relatives à la priorité:
98/11860 23 septembre 1998 (23.09.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F-92100 Boulogne (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: CHEVREAU, Sylvain [FR/FR]; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR). FURON, Teddy [FR/FR]; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(74) Mandataire: KOHRS, Martin; Thomson Multimedia, 46, quai Alphonse Le Gallo, F-92648 Boulogne (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: COPY PROTECTION METHOD FOR DIGITAL DATA STORED ON A MEDIUM

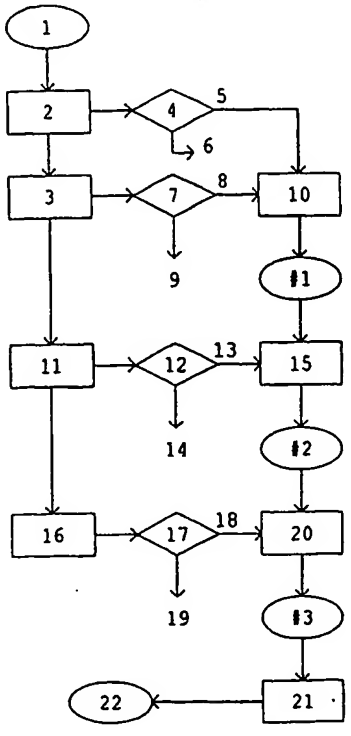
(54) Titre: PROTECTION CONTRE LA COPIE DE DONNEES NUMERIQUES STOCKEES SUR UN SUPPORT D'INFORMATIONS

(57) Abstract

The invention concerns a copy protection method for digital data stored on a medium (1) which consists, on the basis of a first digital data encryption identification (2) and a second digital data tattooing identification (3), in determining a first mark (#1) if the encryption and the tattooing have been identified (5, 8). A third identification of a type of storage medium (11) is followed by the determination (15) of a second mark (#2) if the first mark (#1) has been determined and if a type of storage medium has been identified (13). A fourth identification of cryptographic signature data (16) accompanying the digital data is followed by the determination (20) of a third mark (#3) if the second mark (#2) has been determined and if a cryptographic signature data has been identified (18). Permission for making a digital copy (22) of the digital data is then granted if the third mark (#3) has been determined.

(57) Abrégé

Une méthode de protection contre la copie de données numériques stockées sur un support d'informations (1) prévoit à partir d'une première identification d'un chiffrage (2) des données numériques et d'une seconde identification d'un tatouage (3) de données numériques de déterminer (10) une première marque (#1) si le chiffrage et le tatouage ont pu être identifiés (5, 8). Une troisième identification d'un type du support d'informations (11) est suivie de la détermination (15) d'une seconde marque (#2) si la première marque (#1) a pu être déterminée et si un type déterminé de support d'informations a pu être identifié (13). Une quatrième identification de données de signature cryptographique (16) accompagnant les données numériques est suivie de la détermination (20) d'une troisième marque (#3) si la seconde marque (#2) a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée (18). Une permission de copie numérique (22) des données numériques est délivrée si la troisième marque (#3) a pu être déterminée.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROTECTION CONTRE LA COPIE DE DONNEES NUMERIQUES STOCKEES SUR UN SUPPORT D'INFORMATIONS

L'invention concerne une méthode et un dispositif permettant de protéger contre la copie de données numériques stockées sur un support d'informations.

Une possibilité inhérente aux données numériques est qu'elles peuvent être copiées sans perte notable de qualité puisque la copie consiste à transmettre de la source à l'enregistreur une série de « 1 » et de « 0 ». Le plus grand nombre d'erreurs survenant éventuellement lors de la copie peuvent être palliées en utilisant des méthodes de correction d'erreur. Ainsi lorsqu'un support d'informations contient des données numériques, il est en principe relativement simple d'enregistrer à l'identique sur un support enregistrable le contenu du support d'informations.

De nombreux types et sortes de supports d'informations sont utilisé pour stocker de l'information de toute nature sous forme numérique. Par exemple une bande magnétique, un disque optique enregistrable ou non (CD, CD-R, CD-RW, DVD, DVD-R, disque Magneto-optique etc., respectivements de l'anglais Compact Disc, CD-Recordable, CD-Read Write, Digital Versatile Disc, DVD-Recordable) peut stocker de l'information audio et / ou vidéo sous forme numérique.

Afin de mieux préserver par exemple les intérêts des auteurs de l'information stockée ou ceux de producteurs de support d'informations préenregistré, il est désirable de limiter les possibilités de copier librement et simplement les données numériques. Divers mécanismes et possibilités existent actuellement pour protéger des données numérique contre une copie illégitime.

De façon connue les données numériques peuvent être chiffrées lorsqu'elles sont stockées sur le support d'informations. Le chiffrage permet de limiter l'utilisation des données numériques au détenteur d'une clé publique ou privée de déchiffrage. Le chiffrage est par exemple utilisé dans la protection de données sur les DVD, disques optiques utilisés pour stocker des données vidéo sous forme numérique. Ainsi un lecteur de DVD nécessite une clé appropriée pour déchiffrer les données lues sur le DVD.

Une façon de protéger des données numériques contre la copie consiste à les doter d'un tatouage, c'est-à-dire de données auxiliaires attachées aux données numériques. Le tatouage doit être non-modifiable et non effaçable. La lecture des données se fait à l'aide d'une clé publique qui identifie le tatouage.

La clé publique est un code bien connu par le public, ou plus précisément contenu dans la plupart des lecteurs de supports d'informations. Lors d'une éventuelle copie des données numériques tatouées, une clé privée est requise pour remettre en place le tatouage sur la copie, sans quoi la copie devient illégale puisque dépourvue de tatouage. La clé privée est détenue par l'auteur ou le producteur de l'information ainsi tatouée. Les données numériques copiées sans tatouage ne sont plus lues par le lecteur car celui-ci n'identifie pas de tatouage là où il devrait en trouver un. Ainsi le tatouage ne permet pas de faire de copie sans la clé privée. Si une copie est nécessaire alors l'enregistreur doit intégrer cette clé privée.

Le tatouage n'empêche pas la copie par voie analogique des données numériques, c'est-à-dire une copie qui nécessiterait d'abord une conversion des données numériques en signal analogique et qui prendrait le signal analogique comme source pour la copie.

Une solution connue pour éviter la copie d'un support numérique par voie analogique et plus particulièrement dans le domaine de la vidéo et de la télévision consiste à altérer le signal analogique de telle façon qu'il puisse être utilisé pour afficher une image sur l'écran d'un téléviseur par le biais d'une entrée analogique de ce téléviseur, mais que le même signal ne soit pas utilisable pour faire une copie avec un magnétoscope. Plus précisément un circuit électronique est employé pour influer sur des paramètres de synchronisation de l'image. Ces paramètres de synchronisation sont perçus différemment par un téléviseur et par un magnétoscope. Cette solution ne permet pas d'empêcher la copie numérique de données numériques.

Une autre solution pour limiter les copies numériques de données numériques consiste à doter celles-ci d'informations de gestion des générations. En principe cette information véhicule l'information « ne jamais copier » pour des données qui n'ont pas le droit d'être copiées et l'information « copie » ou « copie numéro X » si les données sont une copie de première ou x-ième génération d'un original. Ainsi un enregistreur peut à l'aide de ces informations savoir si les données numériques à copier ont le droit d'être copiées numériquement et empêcher la copie si elle est interdite pour la 2ième ou (X+1)ième génération. A chaque copie l'information de gestion des générations est mise à jour. Cette manipulation de l'information de gestion des générations la rend vulnérable à être faussée. En effet l'information de gestion des générations est à un stade de la copie disponible en clair c'est-à-dire sous forme déchiffrée. La manipulation nécessite aussi que l'enregistreur numérique soit équipé en conséquence.

L'information de gestion des générations ne permet pas d'éviter en soi les copies par voie analogique.

Un objet de l'invention consiste à trouver une solution de protection contre la copie numérique dans laquelle aucune information relative à la génération de copie est disponible en clair lors de la copie.

Un autre objet de l'invention consiste à trouver une solution dans laquelle aucune modification de données relatives à la protection contre la copie soit entreprise à l'enregistrement éventuelle d'une copie.

Une solution que propose l'invention prévoit une méthode de protection contre la copie de données numériques stockées sur un support d'informations, comprenant

une première identification d'un chiffrage des données numériques,

une seconde identification d'un tatouage de données numériques,

une première détermination d'une première marque si le chiffrage et le tatouage ont pu être identifiés,

une troisième identification d'un type du support d'informations,

une seconde détermination d'une seconde marque si la première marque a pu être déterminée et si un type déterminé de support d'informations a pu être identifié,

une quatrième identification de données de signature cryptographique accompagnant les données numériques,

une troisième détermination d'une troisième marque si la seconde marque a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée,

une première délivrance d'une permission de copie numérique des données numériques si la troisième marque a pu être déterminée.

Une première réalisation avantageuse de l'invention prévoit une seconde délivrance d'une interdiction de lecture des données numériques si la première identification est négative et si le tatouage a pu être identifié, ou si le chiffrage a pu être identifié et la seconde identification est négative.

Une deuxième réalisation avantageuse de l'invention prévoit une troisième délivrance d'une permission de copie numérique des données numériques si la première et la seconde identifications sont négatives.

Une troisième réalisation avantageuse de l'invention prévoit une quatrième délivrance d'une interdiction de copie numérique des données numériques si la première marque a pu être déterminée et si la troisième identification révèle un type différent du type déterminé de support d'informations.

Une quatrième réalisation avantageuse de l'invention prévoit une cinquième délivrance d'une interdiction de copie numérique des données numérique si la deuxième marque a pu être déterminée et si la quatrième identification est négative.

Une cinquième réalisation avantageuse de l'invention prévoit une conversion des données numériques en signaux analogiques et une altération des signaux analogiques si la première, la quatrième ou la cinquième délivrance a été réalisée.

Une sixième réalisation avantageuse de l'invention prévoit que l'interdiction de copie numérique comprend une suppression de sortie des données numériques.

Une septième réalisation avantageuse de l'invention prévoit un déchiffrage des données numériques si un chiffrage a pu être identifié afin d'obtenir des données numériques déchiffrées et des données de signature cryptographique déchiffrées, un premier chiffrage des données de signature cryptographique à l'aide d'un clé publique pour obtenir des données de signature cryptographique rechiffrée, et un second chiffrage des données numériques déchiffrées à l'aide d'une clé privée pour obtenir des données numériques rechiffrées.

Une autre solution que propose l'invention prévoit un dispositif de lecture de données numériques stockées sur un support d'informations comprenant au moins,

une sortie numérique permettant de livrer des signaux représentatifs des données numériques lors d'une lecture des données numériques,

une sortie analogique permettant de livrer des signaux analogiques représentatifs des données numériques lors d'une lecture des données numériques,

un système de déchiffrage pour les données numériques permettant notamment d'établir si les données numériques sont chiffrées et si oui de déchiffrer les données numériques chiffrées, d'identifier si les données numériques comportent un tatouage et/ou des données de signature cryptographique, et d'identifier un type du support d'informations,

un système de protection pour la copie des données numériques recevant des signaux du système de déchiffrage pour les évaluer, et générant un signal de permission de copie dans le cas où les données numériques sont chiffrées, ont un tatouage, sont sur une support de type non-enregistrable et possèdent des données de signature cryptographique,

une partie de contrôle de l'enregistrement qui permet de gérer un flux de données numériques vers la sortie numérique lorsqu'elle reçoit notamment un signal de permission de copie,

un système de protection pour la lecture recevant des signaux du système de déchiffrage et générant un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées, ou lorsque les données numériques sont chiffrées mais non tatouées,

une partie de contrôle de la lecture qui permet d'interrompre la lecture des données ou leur sortie vers la sortie analogique lorsqu'elle reçoit notamment un signal d'interdiction de lecture.

Dans la suite, des exemples de réalisation sont présentés qui permettront d'illustrer et de mieux comprendre l'invention, en faisant référence aux figures 1 à 8, brièvement décrites ci-dessous :

Fig. 1 contient un organigramme illustrant un mode de réalisation de l'invention,

Fig. 2 à 5 contiennent des organigrammes illustrant des aspects de l'invention,

Fig. 6 contient un organigramme illustrant une conversion numérique-analogique selon l'invention,

Fig. 7 contient un organigramme illustrant des aspects de l'invention relatifs au chiffrage,

fig. 8 contient un schéma illustrant un dispositif selon l'invention.

La Fig. 1 contient un organigramme dans lequel des données numériques stockées sur un support d'informations 1 sont soumises à une première identification d'un chiffrage 2 afin de vérifier si les données numériques sont stockées sous forme chiffrée, puis à une seconde identification d'un tatouage 3 pour voir si les données sont pourvues d'un tatouage numérique. Une première bifurcation 4 permet de distinguer les cas où un chiffrage est identifié 5 ou non 6. Une seconde bifurcation 7 permet de distinguer les cas où un tatouage est identifié 8 ou non 9. Si les cas 5 et 8 sont vérifiés une première détermination 10 génère une première marque #1.

Une troisième identification 11 d'un type du support d'informations 1 sert à voir si le support d'informations est par exemple du type non-enregistrable ou enregistrable. Une information sur le type peut être contenue dans les données numériques en soi où résulter de mesures physiques de paramètres du support d'informations 1 lors par exemple d'une initialisation dans un lecteur du support d'informations 1. Une troisième bifurcation 12 permet de distinguer les cas où le

type serait d'un type déterminé 13, par exemple un support d'informations non enregistrable tel qu'un disque optique pressé, ou non 14. Si le cas 13 est vérifié et la première marque #1 a été générée alors une seconde détermination 15 génère une seconde marque #2.

Une quatrième identification 16 de données de signature cryptographique vérifie si les données numériques possèdent une signature cryptographique. Une quatrième bifurcation 17 permet de distinguer les cas où la signature cryptographique est présente 18 ou non 19. Si le cas 18 est vérifié et la seconde marque #2 a été générée alors une troisième détermination 20 génère une troisième marque #3.

En présence de la troisième marque #3 une première délivrance 21 d'une permission de copie numérique 22 des données numériques est réalisée.

Globalement l'organigramme de la Fig. 1 montre comment divers critères afférents aux données numériques mais aussi au support d'informations peuvent mener à la délivrance d'une permission de copie numérique, l'idée étant de ne permettre une copie que dans des condition définies. Par exemple les données ne doivent pas avoir été manipulée donc doivent être chiffrée et tatouées. Ensuite les données ne doivent pas encore avoir été copiées. Si les données sont sur un disque non-enregistrable alors a priori les données sont sur un support d'informations d'origine. Finalement les données doivent posséder une signature cryptographique. Celle-ci indique que les données peuvent être copiées. C'est alors que les données reçoivent la permission de copie numérique. Un résultat de la copie des données sera identique à l'original sauf en ce qui concerne le support d'informations qui devra être enregistrable. Une nouvelle copie des données à partir du support d'informations enregistrable serait impossible car la deuxième marque #2 ne pourrait être générée après la troisième identification 11. En effet la troisième bifurcation 12 nous mènerait dans le cas 14.

D'autres cas de figure sont à envisager lorsque par exemple le chiffrage ou le tatouage des données numériques ne peuvent être identifiés. Normalement le chiffrage et le tatouage vont de pairs et l'absence de l'un ou de l'autre est un indice de manipulation illicite des données numériques. Il s'agit alors d'aller plus loin que de simplement interdire la copie des données numériques. Il faut empêcher la lecture de celles-ci.

Un organigramme dans la Fig. 2 illustre deux cas de figure où le chiffrage et le tatouage ne sont pas identifiés ensembles. Un cas de figure prévoit que la première bifurcation 4 livre le cas 6, c'est-à dire que la première identification d'un chiffrage est négative, et que la seconde bifurcation 7 livre le

cas 8, c'est-à dire qu'un tatouage est présent. Alors une seconde délivrance 23 génère une interdiction de lecture des données numériques 24. En pratique cela pourrait par exemple conduire à une interruption de la lecture des données. Un autre cas de figure prévoit que la première bifurcation 4 livre le cas 5, c'est-à dire qu'un chiffrage est identifié, et que la seconde bifurcation 7 livre le cas 9, c'est -à dire que la seconde identification d'un tatouage est négative. Dans cet autre cas la seconde délivrance génère l'interdiction de lecture 24.

La méthode décrite permet de copier librement des données numériques qui ne sont pas protégées, par exemple des données dépourvues de chiffrage et de tatouage. La Fig. 3 contient un organigramme dans lequel la première et la seconde bifurcation 4 et 7 livrent chacune un cas d'identification négative respectivement les cas 6 pour le chiffrage et 9 pour le tatouage. Une troisième délivrance 25 génère alors directement la permission de copie numérique 22.

Dans le dernier cas il importe peut que les données soient sur un support d'informations enregistrable ou non. L'absence de chiffrage et de tatouage indique un niveau de protection des données minimum.

Dans certains cas de figure les données doivent pouvoir être lues et exploitées mais non copiées. C'est le cas notamment lorsque l'on achète un support d'informations contenant des données numériques dont l'auteur ou le producteur veut éviter la copie. C'est le cas également lorsqu'un support d'informations enregistrable contenant des données copiées légalement est lu. Un tel cas est illustré à l'aide d'un organigramme dans la Fig. 4 où une quatrième délivrance 26 vérifie que la première marque #1 a été délivrée et que le cas 14 d'identification d'un type de support d'informations différent du type déterminé ait eu lieu avant de générer une interdiction de copie 27. En pratique le lecteur devrait mettre en oeuvre un dispositif empêchant une copie des données numériques, par exemple en inhibant une sortie numérique du lecteur.

Un autre tel cas est illustré à l'aide d'un organigramme dans la Fig. 5. Si la deuxième marque #2 est identifiée et le cas 19 signalise une quatrième identification négative, c'est à dire qu'aucune signature cryptographique permettant une copie des données est présente, alors une cinquième délivrance 28 génère l'interdiction de copie 27.

Il est entendu que le fait qu'aucune signature cryptographique permettant une copie des données soit identifié n'exclut pas la présence d'une signature cryptographique particulière interdisant la copie.

Tout au long de la description il a déjà été fait mention du fait que le support d'informations 1 est utilisé dans un lecteur approprié. Les données numériques stockées sur le support d'informations 1 peuvent être dans certains cas acheminées vers une sortie numérique du lecteur. Dans l'exemple d'un lecteur DVD (disque optique pour données numériques vidéo/audio), une sortie numérique peut être prévue pour sortir un signal représentatif des données vers un lecteur / enregistreur DVD-R (ou autre) au fins d'une copie, ou vers un ordinateur pour faire du traitement d'images. En général le lecteur prévoit aussi une sortie analogique afin de pouvoir transmettre un signal analogique représentatif des données numériques vers l'entrée analogique par exemple d'un téléviseur.

Un organigramme dans la Fig. 6 indique par une flèche pointillée que le support d'informations livre des données numériques 29. Une conversion 30 permet de convertir les données numériques 29 en signaux analogiques 31. Une présence de la permission de copie numérique 22 ensemble avec l'une quelconque des première, seconde ou troisième marques (#1, #2, #3), ou une présence de l'interdiction de copie numérique 27, est détectée dans une détection 32 qui le cas échéant déclenche une altération 33 des signaux analogiques pour obtenir des signaux analogiques altérés 34. Les signaux analogiques sont par exemple altérés de façon à ce qu'ils puissent être utilisés pour obtenir des images sur un téléviseur mais qu'il soit impossible de les copier à l'aide d'un magnétoscope à entrée analogique.

Avantageusement il est prévu une suppression à une sortie numérique du lecteur des données numériques 35 en présence de l'interdiction de copie numérique 27.

Le chiffrage des données numériques sur le support d'informations se fait normalement du coté du producteur. Le chiffrage se fait à l'aide d'un algorithme de chiffrage et d'une clé privée que seul le producteur détient. Le chiffrage est conçu de telle façon qu'il est possible de déchiffrer les données à l'aide d'une clé publique largement répandue. Lors du déchiffrage des données, la partie concernant la signature cryptographique est bien sûr également déchiffrée et nécessite d'être rechiffrée sans toutefois être modifiée avant d'être transmise à une sortie numérique pour copie. Afin de limiter les risques de piratage d'une clé privée, le lecteur ne contient pas cette clé privée et rechiffre la signature cryptographique à l'aide d'une clé publique. La Fig. 7 contient un organigramme dans lequel le support d'informations 1 est source de données numériques 29. Un déchiffrage 36 permet d'obtenir des donnée numériques déchiffrées 37 et une

signature cryptographique déchiffrée 38. Cette dernière est chiffrée lors d'un premier chiffrage 39 à l'aide d'une clé publique 40 contenue dans le lecteur avant d'être acheminée sous forme de signature cryptographique chiffrée 41 vers une sortie numérique (non illustrée) ensemble avec les données numériques chiffrées 411 lors d'un second chiffrage 399 à l'aide de la clé privée 400. Ainsi aucune manipulation des données et du tatouage n'est possible.

Un dispositif de lecture de données numériques 42 illustré à la Fig. 8 comprend une sortie numérique 43 qui permet de livrer des signaux représentatifs des données numériques lors d'un lecture des données numérique d'un support d'informations. Cette sortie 43 peut par exemple être réalisée à l'aide d'un bus numérique au standard IEEE1394. Une sortie analogique 44 permet de livrer des signaux analogiques représentatifs des mêmes données numériques. Un système de déchiffrage 45 permet de déchiffrer des données numériques si celles-ci sont chiffrées, mais aussi d'identifier un éventuel tatouage et des données de signature cryptographique. Le système de déchiffrage permet de mettre en oeuvre par exemple les identifications 2, 3, 11 et 16 de la méthode illustrée à la Fig. 1.

Un système de protection pour la copie des données numériques 46 utilise des signaux émis par le système de déchiffrage 45 et les évalue en implémentant les déterminations 10, 15 et 20 de la méthode illustrée à la Fig. 1, et délivre après avoir déterminé les marques #1, #2 et #3 un signal de permission de copie.

Une partie de contrôle de l'enregistrement 47 permet de gérer un flux de données numériques vers la sortie numérique. Cette partie peut notamment activer le flux lorsqu'elle obtient du système de protection 46 le signal de permission de copie.

Le système de protection pour la copie des données numériques 46 peut également jouer le rôle d'un système de protection pour la lecture. Ce dernier système génère à l'aide des signaux reçus du système de déchiffrage 45 un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées ou encore lorsque les données numériques sont chiffrées mais non tatouées.

Une partie de contrôle de la lecture 48 permet d'interrompre la lecture des données numériques lorsqu'elle reçoit le signal d'interdiction du système de protection pour la lecture.

Liste des références

1. support d'informations
2. première identification d'un chiffrage
3. seconde identification d'un tatouage
4. première bifurcation
5. chiffrage identifié
6. chiffrage non identifié
7. seconde bifurcation
8. tatouage identifié
9. tatouage non identifié
10. première détermination

#1. première marque

11. troisième identification d'un type de support d'informations
12. quatrième bifurcation
13. type déterminé
14. pas le type déterminé
15. seconde détermination

#2. seconde marque

16. quatrième identification de données de signature cryptographique
17. quatrième bifurcation
18. signature cryptographique présente
19. signature cryptographique non présente
20. troisième détermination

#3. troisième marque

21. première délivrance
22. permission de copie numérique
23. seconde délivrance
24. interdiction de lecture des données numériques
25. troisième délivrance
26. quatrième délivrance
27. interdiction de copie
28. cinquième délivrance
29. données numérique
30. conversion
31. signaux analogiques

32. détection
33. altération
34. signaux analogiques altérés
35. suppression de sortie des données numériques
36. déchiffrage des données numériques
37. données numériques déchiffrées
38. données de signature cryptographique déchiffrées
39. premier chiffrage
399. second chiffrage
40. clé publique
400. clé privée
41. signature cryptographique chiffrée
411. données numériques chiffrées
42. dispositif de lecture de données numériques
43. sortie numérique
44. sortie analogique
45. système de déchiffrage
46. système de protection pour la copie des données numériques
47. partie de contrôle de l'enregistrement
48. partie de contrôle de la lecture.

Revendications

1. Une méthode de protection contre la copie de données numériques stockées sur un support d'informations (1), comprenant

une première identification d'un chiffrage (2) des données numériques,

une seconde identification d'un tatouage (3) des données numériques,

caractérisée en que la méthode comprend en outre

une première détermination (10) d'une première marque (#1) si le chiffrage et le tatouage ont pu être identifiés (5, 8),

une troisième identification d'un type du support d'informations (11),

une seconde détermination (15) d'une seconde marque (#2) si la première marque (#1) a pu être déterminée et si un type déterminé de support d'informations a pu être identifié (13),

une quatrième identification de données de signature cryptographique (16) accompagnant les données numériques,

une troisième détermination (20) d'une troisième marque (#3) si la seconde marque (#2) a pu être déterminée et si une donnée de signature cryptographique a pu être identifiée (18),

une première délivrance (21) d'une permission de copie numérique (22) des données numériques si la troisième marque (#3) a pu être déterminée.

2. Une méthode de protection selon la revendication 1, caractérisée en ce qu'elle comprend

une seconde délivrance (23) d'une interdiction de lecture (24) des données numériques si la première identification est négative (6) et si le tatouage a pu être identifié (8), ou si le chiffrage a pu être identifié (5) et la seconde identification est négative (9).

3. Une méthode de protection selon l'une quelconque des revendications 1 ou 2, caractérisée en ce qu'elle comprend

une troisième délivrance (25) d'une permission de copie numérique (22) des données numériques si la première (6) et la seconde (9) identifications sont négatives.

4. Une méthode de protection selon l'une quelconque des revendications 1 à 3, caractérisée en ce qu'elle comprend

une quatrième délivrance (26) d'une interdiction de copie (27) numérique des données numériques si la première marque (#1) a pu être déterminée et si la troisième identification révèle un type différent (14) du type déterminé de support d'informations.

5. Une méthode de protection selon l'une quelconque des revendications 1 à 4, caractérisée en ce qu'elle comprend

une cinquième délivrance (28) d'une interdiction de copie (27) numérique des données numériques si la deuxième marque (#2) a pu être déterminée et si la quatrième identification est négative (19).

6. Une méthode de protection selon l'une quelconque des revendications 1, 4 ou 5, caractérisée en ce qu'elle comprend

une conversion (30) des données numériques (29) en signaux analogiques (31),

une altération (33) des signaux analogiques si la première (21), la quatrième (26) ou la cinquième délivrance (28) a été réalisée.

7. Une méthode de protection selon l'une quelconque des revendications 4 ou 5, caractérisée en ce que l'interdiction de copie numérique (27) comprend une suppression (35) de sortie des données numériques.

8. Une méthode de protection selon la revendication 1, caractérisée en ce qu'elle comprend

un déchiffrage des données numériques (36) si un chiffrage a pu être identifié afin d'obtenir des données numériques déchiffrées (37) et des données de signature cryptographique déchiffrées (38),

un premier chiffrage (39) des données de signature cryptographique à l'aide d'une clé publique (40).

9. Une méthode de protection selon la revendication 8, caractérisé en ce qu'elle comprend

un second chiffrage (399) des données numériques déchiffrées à l'aide d'une clé privée (400).

10. Un dispositif de lecture de données numériques stockées sur un support d'informations comprenant au moins,

une sortie numérique (43) permettant de livrer des signaux représentatifs des données numériques lors d'une lecture des données numériques,

une sortie analogique (44) permettant de livrer des signaux analogiques représentatifs des données numériques lors d'une lecture des données numériques,

un système de déchiffrage (45) pour les données numériques permettant notamment d'établir si les données numériques sont chiffrées et si oui de déchiffrer les données numériques chiffrées, d'identifier si les données numériques comportent un tatouage et/ou des données de signature cryptographique, et d'identifier un type du support d'informations,

un système de protection (46) contre la copie de données numériques recevant des signaux du système de déchiffrage pour les évaluer, et générant un signal de permission de copie dans le cas où les données numériques sont chiffrées, ont un tatouage, sont sur un support de type non-enregistrable et possèdent des données de signature cryptographique,

une partie de contrôle (47) de l'enregistrement qui permet de gérer un flux de données numériques vers la sortie numérique lorsqu'elle reçoit notamment un signal de permission de copie,

un système de protection pour la lecture recevant des signaux du système de déchiffrage et générant un signal d'interdiction de lecture lorsque les données numériques ne sont pas chiffrées mais tatouées, ou lorsque les données numériques sont chiffrées mais non tatouées,

une partie de contrôle de la lecture (48) qui permet d'interrompre la lecture des données ou leur sortie vers la sortie analogique lorsqu'elle reçoit notamment un signal d'interdiction de lecture.

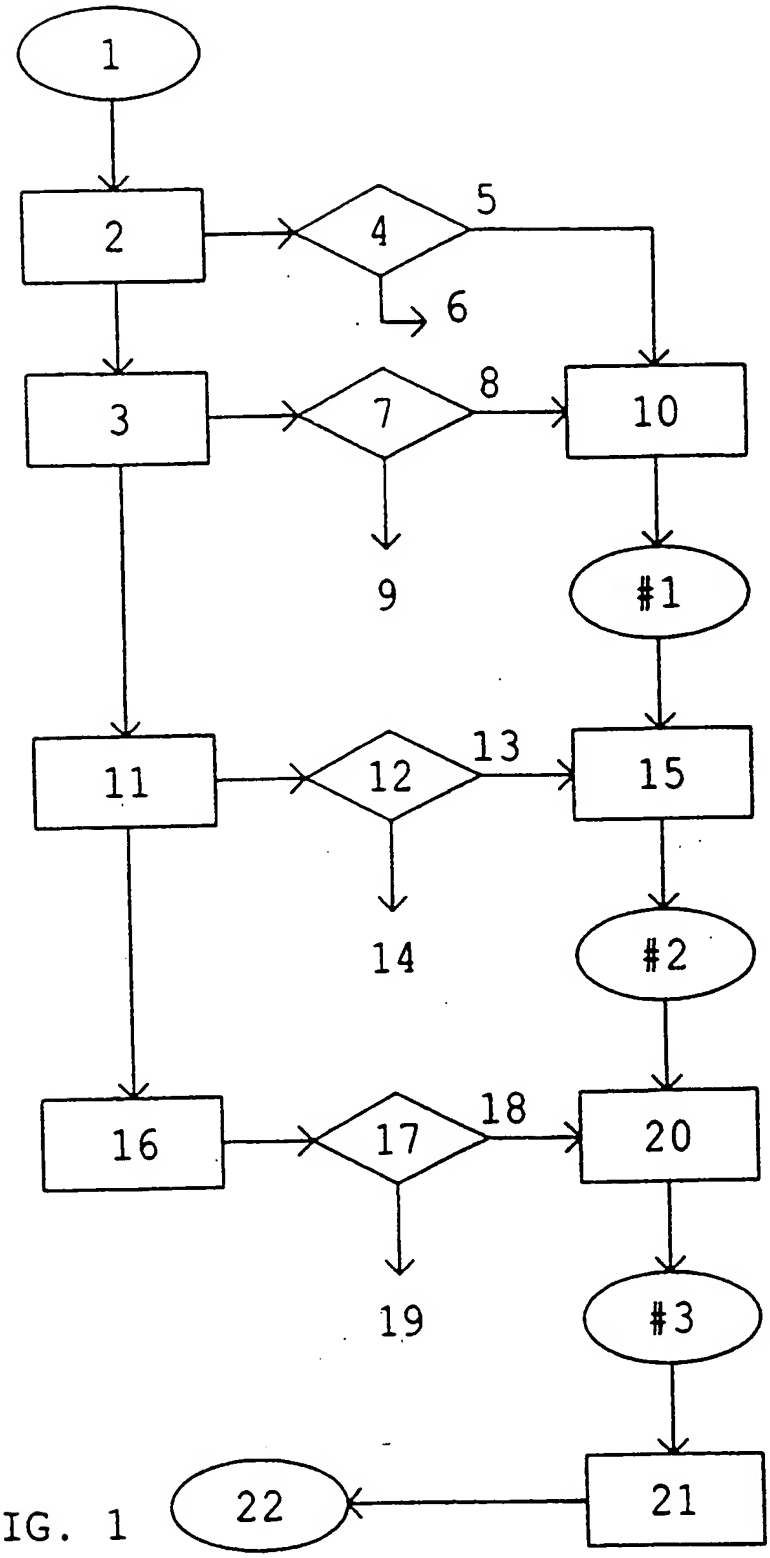


FIG. 1

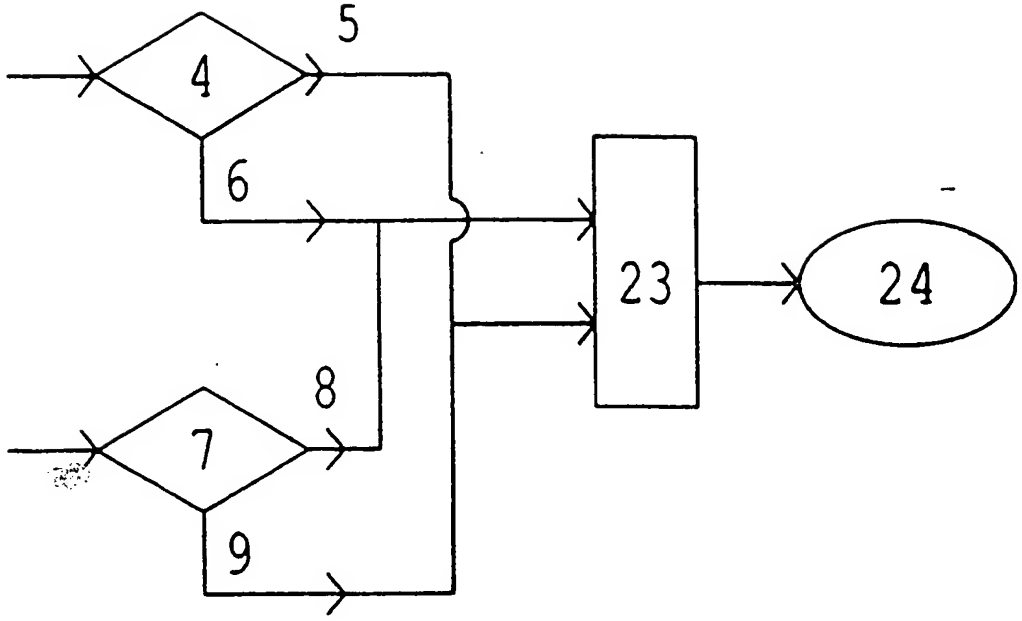


FIG. 2

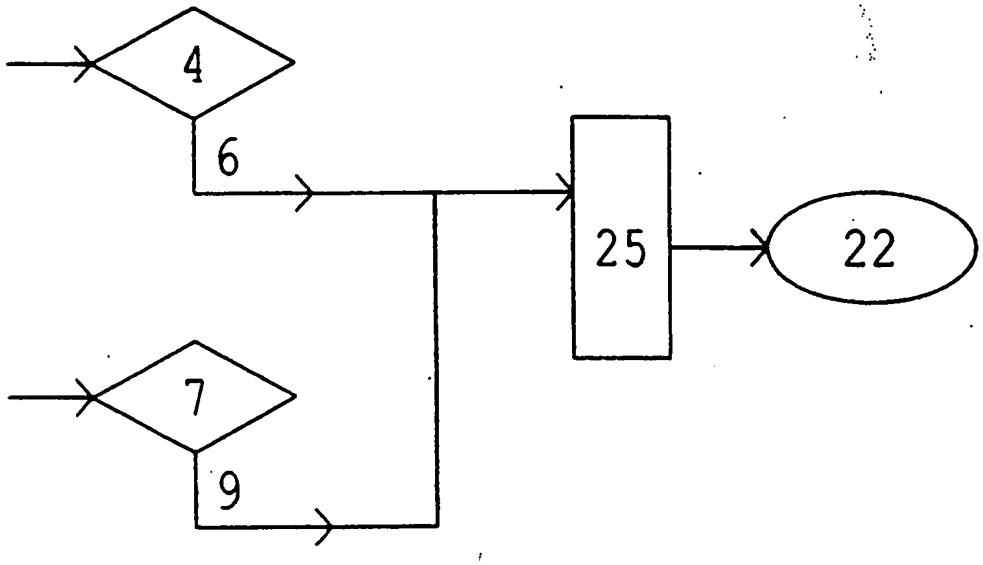


FIG. 3

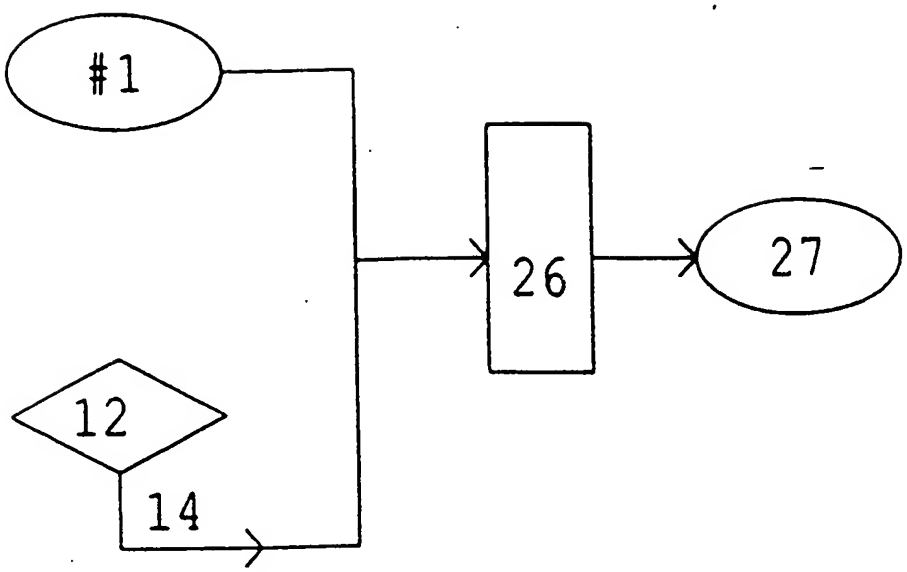


FIG. 4

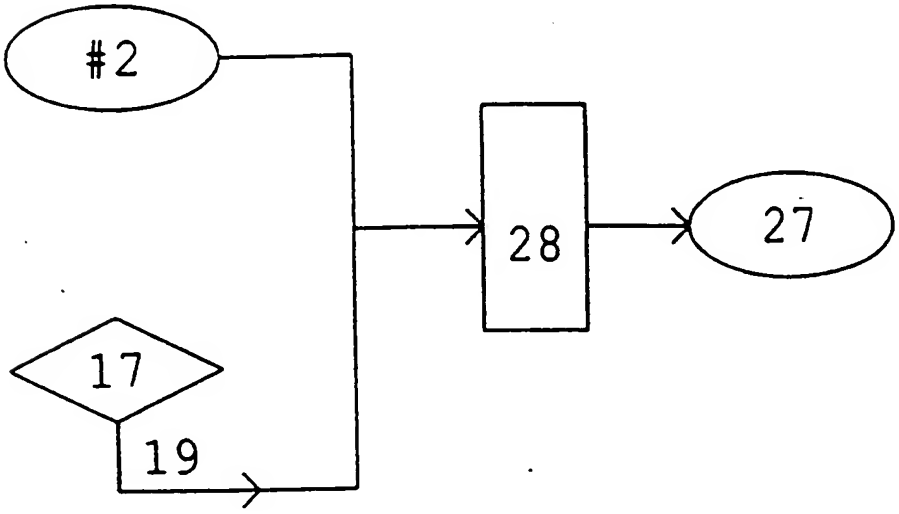


FIG. 5

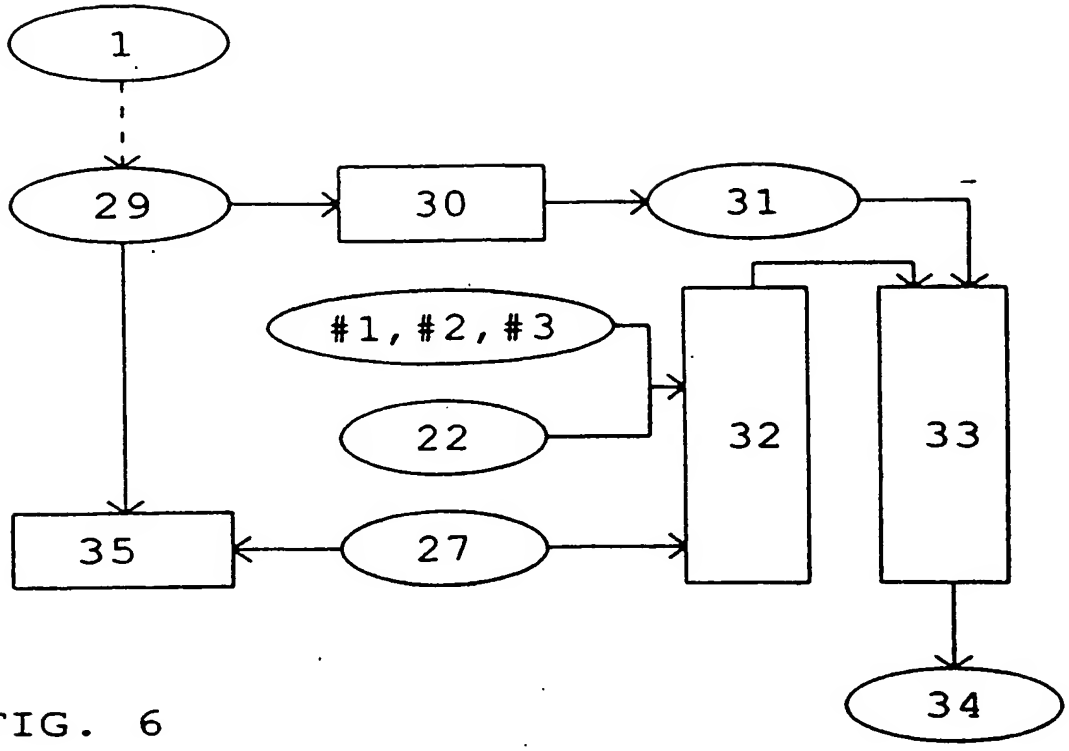


FIG. 6

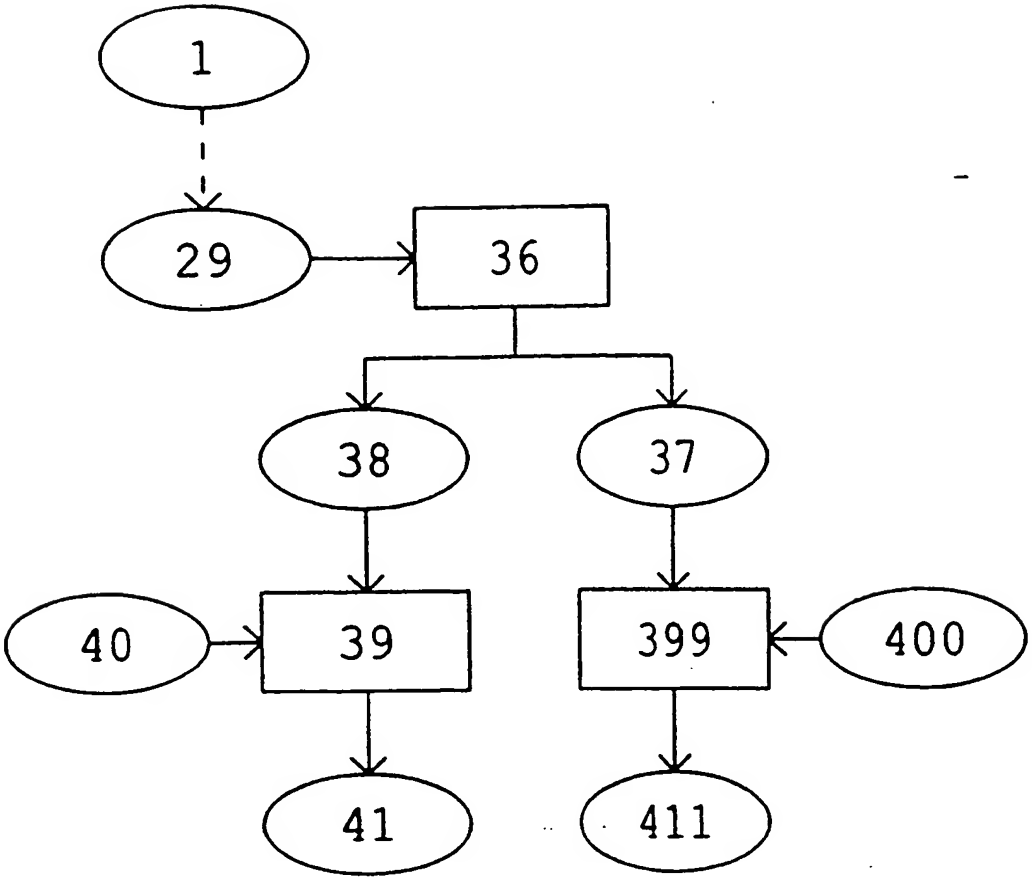


FIG. 7

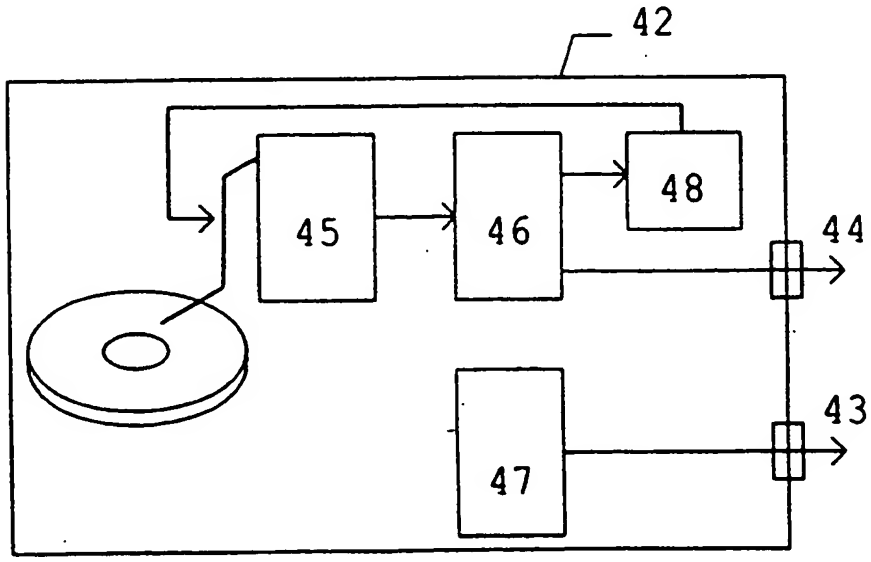


FIG. 8

INTERNATIONAL SEARCH REPORT

Inter ional Application No
PCT/FR 99/02267

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 413 350 A (TOKYO SHIBAURA ELECTRIC CO) 20 February 1991 (1991-02-20) abstract column 2, line 30 -column 3, line 25 column 5, line 23 -column 9, line 5 figures 1-4 ---	1-5,10
A	US 4 937 679 A (RYAN JOHN O) 26 June 1990 (1990-06-26) abstract; figure 1 column 3, line 2 - line 60 ---	1,10
A	EP 0 416 663 A (MATSUSHITA ELECTRIC IND CO LTD) 13 March 1991 (1991-03-13) abstract column 4, line 40 -column 5, line 13 claims 1,3; figure 2 --- -/--	1,5-7,10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 1999	12/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schiwy-Rausch, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/FR 99/02267

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 735 752 A (SONY CORP) 2 October 1996 (1996-10-02)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/FR 99/02267

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0413350 A	20-02-1991	JP 1861103 C	08-08-1994
		JP 3075827 A	29-03-1991
		JP 5070176 B	04-10-1993
		DE 69032305 D	18-06-1998
		DE 69032305 T	08-10-1998
		US 5295187 A	15-03-1994
US 4937679 A	26-06-1990	US 5130810 A	14-07-1992
		AT 122835 T	15-06-1995
		DE 68922658 D	22-06-1995
		DE 68922658 T	19-10-1995
		EP 0348218 A	27-12-1989
		ES 2072300 T	16-07-1995
		HK 1002419 A	21-08-1998
		JP 2064947 A	05-03-1990
		KR 9406160 B	08-07-1994
		PH 26068 A	29-01-1992
		AT 96933 T	15-11-1993
		DE 3788020 D	09-12-1993
		DE 3788020 T	03-03-1994
		EP 0256753 A	24-02-1988
		ES 2044937 T	16-01-1994
		HK 1008109 A	30-04-1999
		IE 62247 B	11-01-1995
		JP 2881432 B	12-04-1999
		JP 63107281 A	12-05-1988
		US 4907093 A	06-03-1990
		US 4819098 A	04-04-1989
		US 5194965 A	16-03-1993
EP 0416663 A	13-03-1991	JP 2629372 B	09-07-1997
		JP 3097167 A	23-04-1991
		JP 2584067 B	19-02-1997
		JP 3102676 A	30-04-1991
		DE 69032036 D	19-03-1998
		DE 69032036 T	20-08-1998
		KR 9408688 B	24-09-1994
		US 5159502 A	27-10-1992
EP 0735752 A	02-10-1996	JP 8275127 A	18-10-1996
		AU 709546 B	02-09-1999
		AU 4826396 A	10-10-1996
		BR 9601234 A	06-01-1998
		CA 2172009 A	01-10-1996
		CN 1135142 A	06-11-1996
		US 5778064 A	07-07-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Dem : Internationale No
PCT/FR 99/02267

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G11B20/00 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G11B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 413 350 A (TOKYO SHIBAURA ELECTRIC CO) 20 février 1991 (1991-02-20) abrégé colonne 2, ligne 30 -colonne 3, ligne 25 colonne 5, ligne 23 -colonne 9, ligne 5 figures 1-4	1-5,10
A	US 4 937 679 A (RYAN JOHN O) 26 juin 1990 (1990-06-26) abrégé; figure 1 colonne 3, ligne 2 - ligne 60	1,10
A	EP 0 416 663 A (MATSUSHITA ELECTRIC IND CO LTD) 13 mars 1991 (1991-03-13) abrégé colonne 4, ligne 40 -colonne 5, ligne 13 revendications 1,3; figure 2	1,5-7,10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
30 novembre 1999	12/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schiwy-Rausch, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Dem. ; Internationale No
PCT/FR 99/02267

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visees
A	EP 0 735 752 A (SONY CORP) 2 octobre 1996 (1996-10-02) -----	

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. : Internationale No
PCT/FR 99/02267

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0413350 A	20-02-1991	JP 1861103 C	08-08-1994
		JP 3075827 A	29-03-1991
		JP 5070176 B	04-10-1993
		DE 69032305 D	18-06-1998
		DE 69032305 T	08-10-1998
		US 5295187 A	15-03-1994
US 4937679 A	26-06-1990	US 5130810 A	14-07-1992
		AT 122835 T	15-06-1995
		DE 68922658 D	22-06-1995
		DE 68922658 T	19-10-1995
		EP 0348218 A	27-12-1989
		ES 2072300 T	16-07-1995
		HK 1002419 A	21-08-1998
		JP 2064947 A	05-03-1990
		KR 9406160 B	08-07-1994
		PH 26068 A	29-01-1992
		AT 96933 T	15-11-1993
		DE 3788020 D	09-12-1993
		DE 3788020 T	03-03-1994
		EP 0256753 A	24-02-1988
		ES 2044937 T	16-01-1994
		HK 1008109 A	30-04-1999
		IE 62247 B	11-01-1995
		JP 2881432 B	12-04-1999
		JP 63107281 A	12-05-1988
		US 4907093 A	06-03-1990
		US 4819098 A	04-04-1989
		US 5194965 A	16-03-1993
EP 0416663 A	13-03-1991	JP 2629372 B	09-07-1997
		JP 3097167 A	23-04-1991
		JP 2584067 B	19-02-1997
		JP 3102676 A	30-04-1991
		DE 69032036 D	19-03-1998
		DE 69032036 T	20-08-1998
		KR 9408688 B	24-09-1994
		US 5159502 A	27-10-1992
EP 0735752 A	02-10-1996	JP 8275127 A	18-10-1996
		AU 709546 B	02-09-1999
		AU 4826396 A	10-10-1996
		BR 9601234 A	06-01-1998
		CA 2172009 A	01-10-1996
		CN 1135142 A	06-11-1996
		US 5778064 A	07-07-1998